AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

Claims 1 to 14. (Canceled).

15. (Currently Amended) An encryption system, comprising:

generating a Vernam key via a symmetrical cipher by a hardware processor, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length;

encrypting by an encryptor, via a Vernam key, the message using logic operations of a Vernam cipher;

communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher;

regenerating the Vernam key using the transmitted secret key and variable parameter;

decrypting the message using the regenerated Vernam key;

providing crypto-hardware including at least one of a chipcard and a multifunctional PC interface adapter with built-in special crypto-hardware, the crypto-hardware storing at least one generated Vernam key;

utilizing the at least one generated Vernam key stored in the crypto-hardware by the encryptor; and

wherein the encryptor being capable of coupling to the crypto-hardware, the encryptor ~~including~~ includes at least one of a personal computer, software executable by a computer, and a terminal which implements a Vernam cipher for broad-band applications in software.

16. (Previously Presented) The encryption system according to claim 15, wherein the crypto-hardware is designed as an external crypto-module and wherein the crypto-hardware has an intermediate storage, the intermediate storage storing a reserve of the Vernam key.

17. (Previously Presented) The encryption system according to claim 16, wherein the intermediate storage is disposed in one of the personal computer and the terminal.

18. (Currently Amended) An encryption system, comprising:

a secret key having a defined key length;

a variable parameter having a length which is a function of the defined key length;

a symmetrical cipher;

a Vernam key having a length that is equal to a length of a message to be protected; the Vernam key being generated from the symmetrical cipher encryption of the secret key and the variable parameter, the Vernam key encrypting the message using logic operations from a Vernam cipher;

at least one of a message-transmission path and a secure channel, the message-transmission path being a path over which the encrypted message is communicated, the secure channel being secured by encrypting the secret key and the variable parameter with an asymmetrical cipher, the secure channel being separate from the message-transmission path; and

a crypto-module including a storage space and one of the symmetrical cipher and the asymmetrical cipher, wherein the crypto-module is separate from the encryptor, the storage space is used to store the Vernam key, and any Vernam cipher operations are performed in the encryptor,

wherein the secret key and the variable parameter are communicated over the secure channel and, subsequently, used in regenerating the Vernam key, the regenerated Vernam key decrypting the message; and wherein the encryptor communicates with the crypto-module to utilize the Vernam key.

19. (Previously Presented) The encryption method according to claim 8, wherein the communicating, from a sending point to a receiving point, the secret key and the variable parameter occurs via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher.

20. (Currently Amended) A method for implementing an encryption system, comprising:

generating a Vernam key from a secret symmetrical key and a secret variable parameter, the secret key having a secret key bit length and the secret variable parameter being a random number multiplied by the secret key bit length, the generated Vernam key

having a Vernam key length which is one of equal to and exceeds a message bit length of a message to be encrypted and transmitted;

encrypting via an encryptor using the Vernam key the message using logic operations of a Vernam cipher;

communicating, from a sending point to a receiving point, the secret key and the variable parameter via a secure channel separate from a message transmission path;

regenerating the Vernam key at the receiving point using the transmitted secret key and variable parameter;

decrypting the transmitted message using the regenerated Vernam key communicated to the receiving point;

wherein a plurality of Vernam keys are generated and stored in a storage module, one of a symmetrical cipher and an asymmetrical cipher is installed and stored in the storage module, the storage-module being separate from an encryptor, and wherein encryption operations using the Vernam cipher are performed in the encryptor, the encryptor including a computer, the encryptor communicating with the crypto-hardware in order to utilize the at least one generated Vernam key stored in the crypto-hardware..

21. (Previously Presented) The method according to claim 20, wherein the Vernam key is generated from a symmetrical cipher operated on the secret key and the variable parameter.

22. (Previously Presented) The method according to claim 20, wherein the secret key is a symmetrical key.

23. (Previously Presented) The method according to claim 20, wherein the Vernam cipher is a simple mathematical operation.

24. (Previously Presented) The method according to claim 23, wherein the simple mathematical operation is EXOR.

25. (Previously Presented) The method according to claim 20, wherein the encryptor is a processor.

26. (Previously Presented) The method according to claim 20, wherein the storage module is at least one of a low-speed chipcard, a chipcard, a PCMCIA module, memory in a personal computer, and memory in a terminal.

27. (Previously Presented) The method according to claim 20, wherein the Vernam cipher operations are performed exclusively in the encryptor.

28. (Previously Presented) The method according to claim 20, wherein the storage module is an external crypto-module; and further comprising controlling, via the Vernam cipher, encryption operations in the encryptor.

29. (Previously Presented) The method according to claim 20, wherein the Vernam key is stored in the encryptor.

30. (Previously Presented) The method according to claim 20, wherein for each Vernam cipher operations on message transmission, one of the generated Vernam keys is used, each Vernam key being used only during one message transmission event.